

CLAIMS

What is claimed is:

- 1 1. A method comprising:
 - 2 storing a first list of hardware registers;
 - 3 receiving video data at an application program;
 - 4 receiving a second list of hardware registers from a device driver;
 - 5 determining whether the first list of hardware registers matches the
 - 6 second list of hardware registers; and
 - 7 if so, streaming the video data to a video decoder.
- 1 2. The method of claim 1 further comprising precluding the streaming of the
 - 2 video data to the video decoder if the first list of hardware registers does not
 - 3 match the second list of hardware registers.
- 1 3. The method of claim 1 further comprising:
 - 2 initializing the device driver upon startup of a computer system
 - 3 forwarding the first list of hardware registers from the device driver to a
 - 4 first security module; and
 - 5 verifying, at the first security module, a digital signature of the device
 - 6 driver prior to storing the first list of hardware registers.
- 1 4. The method of claim 3 further comprising encrypting the first list of

2 hardware registers prior to storing the first list of hardware registers.

1 5. The method of claim 1 further comprising:

2 the application program calling an interface upon receiving the video

3 data;

4 the interface requesting the second list of hardware registers from the

5 device driver; and

6 mapping the second list of hardware registers to a virtual resource map

7 that is accessible by the application.

1 6. The method of claim 5 further comprising:

2 the interface calling a second security module to verify the second list of

3 hardware registers; and

4 the second security module calling the first security module in order to

5 verify the virtual resource map.

1 7. The method of claim 6 further comprising verifying, at the second security

2 module, a digital signature of the interface prior to calling the first security

3 module.

1 8. The method of claim 7 wherein the second security module calls the first

2 security module via a secure link.

1 9. A computer system comprising:

2 a player application that receives data content;

3 a decoder that stores and decodes the data content received at the player,
4 the decoder including hardware registers to store the data content;
5 a driver, coupled to the decoder, that allocates the hardware registers
6 within for access by the player application; and
7 a first security module, coupled to the driver, that secures a first list of
8 resources corresponding to the hardware registers to prevent unauthorized
9 access of the data content within the hardware registers.

1 10. The computer system of claim 9 wherein the first security module verifies
2 the integrity of the driver via digital signatures prior to receiving the first list of
3 resources.

1 11. The computer system of claim 9 further comprising an interface, coupled
2 to the player application, the driver and the decoder, that decrypts the content
3 the data content prior to the data content being stored in the hardware registers.

1 12. The computer system of claim 11 wherein the driver verifies the integrity
2 of the interface via digital signatures and public/private key technologies.

1 13. The computer system of claim 11 further comprising a second security
2 module coupled to the interface and the first security module.

1 14. The computer system of claim 13 wherein the second security module
2 receives a second list of resources from the interface whenever the player
3 application is to release the data content from the hardware registers.

3 data to the video decoder if the first list of hardware registers does not match the
4 second list of hardware registers.

1 20. The article of manufacture of claim 18 when executed by a processing
2 unit, further causes the processing unit to:
3 initialize the device driver upon startup of a computer system
4 forward the first list of hardware registers from the device driver to a first
5 security module; and
6 verify, at the first security module, a digital signature of the device driver
7 prior to storing the first list of hardware registers.

1 21. The article of manufacture of claim 20 when executed by a processing
2 unit, further causes the processing unit to encrypt the first list of hardware
3 registers prior to storing the first list of hardware registers.

1 22. The article of manufacture of claim 18 when executed by a processing
2 unit, further causes:
3 the application program to call an interface upon receiving the video data;
4 the interface to request the second list of hardware registers from the
5 device driver; and
6 mapping the second list of hardware registers to a virtual resource map
7 that is accessible by the application.

1 23. The article of manufacture of claim 22 when executed by a processing

2 unit, further causes:
3 the interface to call a second security module to verify the second list of
4 hardware registers; and
5 the second security module to call the first security module in order to
6 verify the virtual resource map.

1 24. The article of manufacture of claim 23 when executed by a processing
2 unit, further causes verifying, at the second security module, a digital signature
3 of the interface prior to calling the first security module.